SMART INDIA HACKATHON 2025

TITLE PAGE

- **Problem Statement ID- SIH25235**
- **Problem Statement Title- Portable log analysis tool for isolated network.**
- **Theme- Offline, Portable Forensics**
- **PS Category- Software**
- **Team ID- 115366**
- **Team Name- Quorum.pkl**

Quorum.pkl

IDEA TITLE

SMART INDIA HACKATHON 2025

Proposed Solution

Analyst-in-a-Box – a portable, offline security analytics platform.

- Runs fully from an encrypted USB on any laptop (no internet or servers).
- Offers enterprise-grade SIEM power for log collection, threat hunting, and forensics.

How It Solves the Problem

- Portable & Offline: Cross-platform app with zero external dependencies.
- Multi-Source Logs: Collects data via SSH and standard protocols.
- Unified Analysis: Parses & correlates diverse logs into one searchable timeline.
- AI-Powered Detection: Built-in TinyML detects anomalies without cloud access.
- Easy Offline Updates: One-click threat intel updates via secure SOUP process.

Innovation & Uniqueness

- True Portability: Full SIEM capability—no servers, no internet.
- Embedded TinyML: On-device AI for real-time threat detection.
- Secure Offline Update Protocol (SOUP): Fast, safe, one-step updates.
- On-the-Fly Aggregation: Real-time log collection across isolated systems.

Secure Offline Update Protocol (SOUP) Workflow

Admin (Internet-Connected System)	Analyst (Air-Gapped Network)
1. Gather Updates: Threat intel feeds, parsing rules, and AI models	4. Import Package: USB drive connected to Sentinel laptop.
2. Bundle & Secure: Create single .sentinelupdate package (encrypted & compressed).	5. Validate Signature: Sentinel verifies digital signature and package integrity.
3. Sign & Transfer: Digitally sign and move package to secure USB.	6. Apply Update: Updates (threat DB, rules, models) applied atomically and safely.

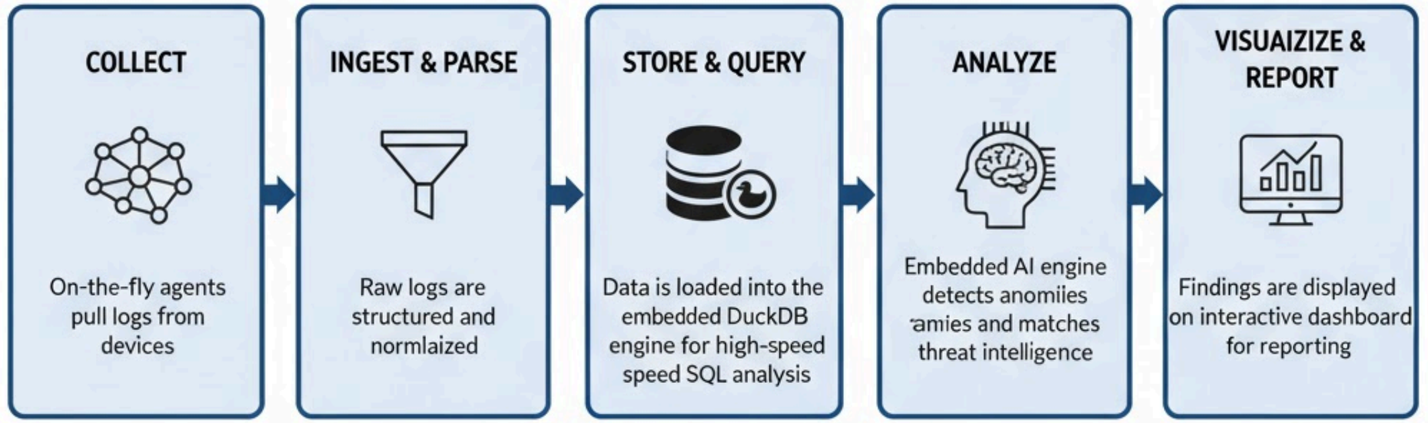
Quorum.pkl

TECHNICAL APPROACH

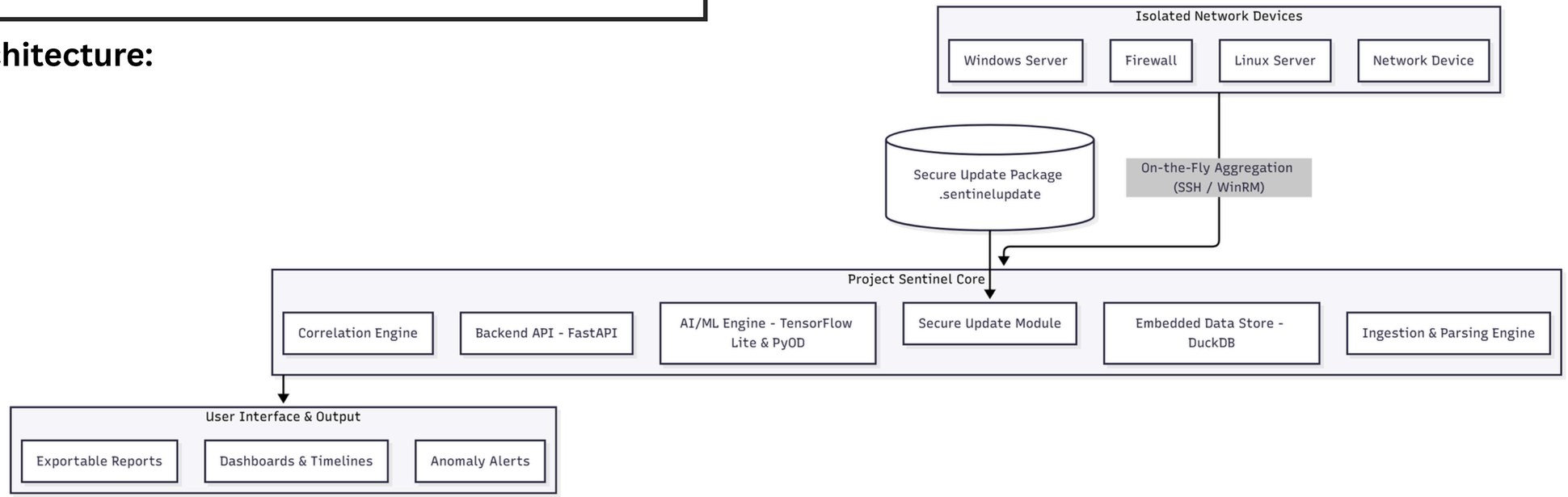
SMART INDIA HACKATHON 2025

Technologies Used

- Backend: Python + FastAPI (async, high-performance API)
- Database: DuckDB (embedded, ultra-fast analytics)
- AI Engine: TensorFlow Lite + PyOD (on-device anomaly detection)
- Frontend: React + Tailwind CSS
- Log Collectors: Python scripts using standard protocols (e.g., SSH)



System Architecture:



Quorum.pkl

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2025

Feasibility Analysis

1. Technical Feasibility

Project Sentinel leverages mature, high-performance open-source technologies, minimizing development risk.

- DuckDB: Serverless, in-process database enabling fast queries on laptops without heavy infrastructure.
- TensorFlow Lite & TinyML: Efficient on-device AI analytics for resource-constrained hardware.

2. Operational Feasibility

The "zero-setup" portable design simplifies deployment in isolated or high-pressure environments.

- Unlike traditional SIEMs requiring clusters or bastion hosts, Project Sentinel is a single executable, ready to use without configuration.

3. Timeline Feasibility

A phased development plan ensures a functional MVP within the hackathon timeline.

- MVP covers log ingestion, parsing, and analysis for key formats (Syslog, EVTX), forming a solid base for future enhancements.

Challenges, Risks & Mitigation Strategies

Challenge	Risk	Mitigation Strategy
Performance on Low-Resource Hardware	Slow analysis may impact investigations	Use DuckDB for fast analytics and TinyML for lightweight AI models
Diverse & Complex Log Formats	Limited support for proprietary logs	MVP supports key formats (Syslog, EVTX); add Custom Parser Editor post-MVP
AI Model Effectiveness	Lower accuracy than cloud models	Hybrid AI Approach combining PyOD + deep learning for balanced detection

Quorum.pkl

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2025

Potential Impact

- Empowers Analysts: Especially in NTRO, defense, and critical infrastructure sectors.
- Transforms Workflow: Converts slow, manual response into fast, intelligence-driven investigation.
- Strengthens Security: Enables standardized, on-site forensics in high-security environments.

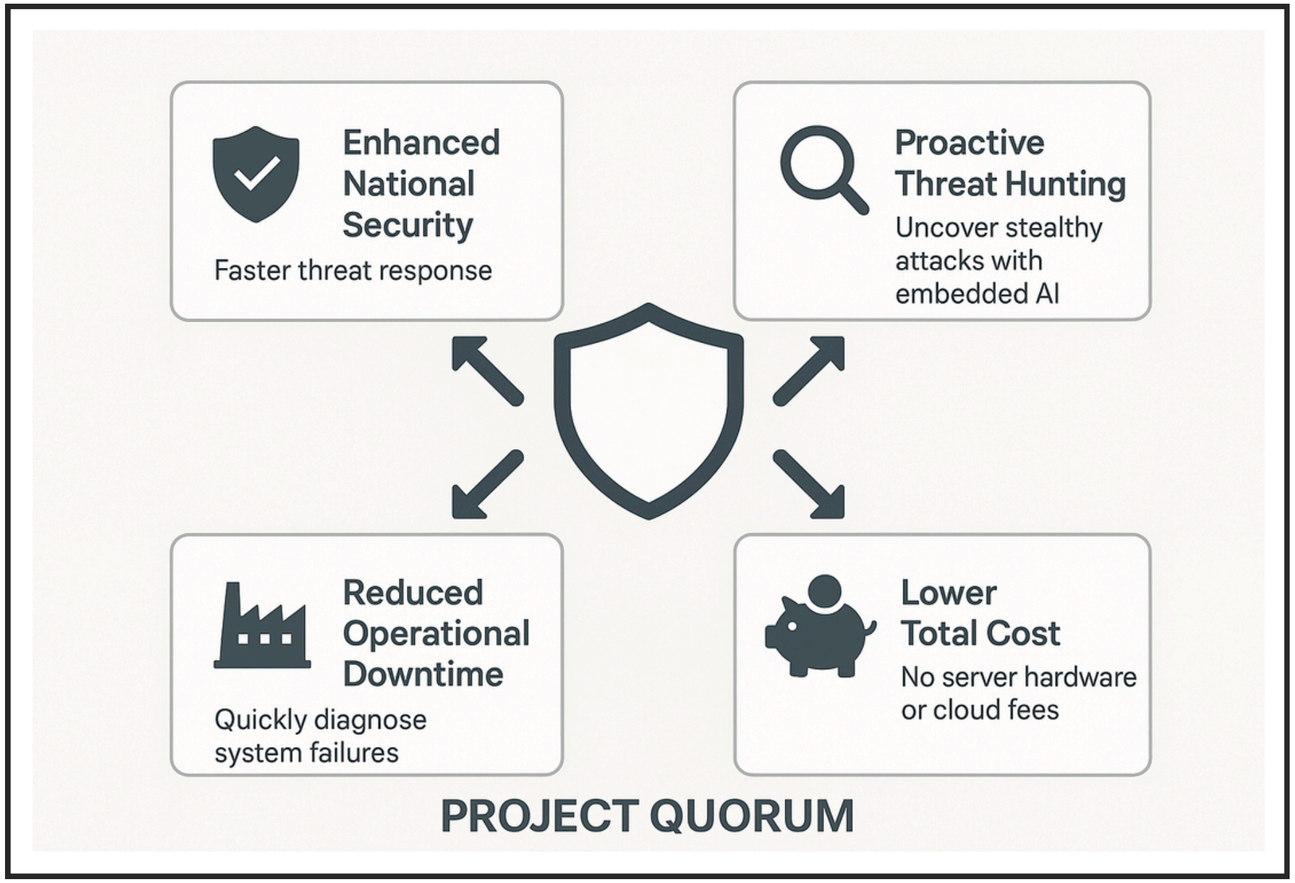
Benefits

National Security:

- Faster incident response in critical networks.
- Proactive detection of APTs and insider threats.
- Maintains forensic integrity with audit-ready evidence trails.

Economic & Operational:

- Reduces infrastructure downtime.
- Boosts analyst productivity via automation.
- Low-cost, serverless, and cloud-free deployment.



Quorum.pkl

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2025

Research & Competitive Analysis

- Existing SIEMs (Splunk, QRadar, ELK): Not suited for portable or offline use; require heavy infrastructure and complex air-gapped setups.
- Lightweight Tools (Graylog, Wazuh, GoAccess): Lack integrated correlation and advanced offline analytics.
- Academic Validation: TinyML research confirms feasibility of on-device AI for intrusion detection; ML studies support automated log parsing and anomaly recognition.
- Technology Proof:
  - DuckDB: High-speed embedded analytics.
  - PyOD / Luminol: Lightweight anomaly detection.
  - TensorFlow Lite: Optimized neural models for laptops and edge devices.

Competitive Landscape: Why Existing Tools Fall Short

Feature	Project Sentinel	Splunk ES	Elastic SIEM	IBM QRadar	Lightweight Tools
Portability	✅ High (Single Executable)	❌ Requires Servers	❌ Server Cluster	❌ Appliance-Based	✅ High
Offline-First	✅ Core Design	❌ No	❌ No	❌ No	✅ Partial
Update Complexity	🔒 Low (Secure Package)	⚠️ High (Manual)	⚠️ High (Manual)	⚠️ High (Bastion)	N/A
Embedded AI/ML	🤖 Yes (TinyML)	⚙️ Server-Based	⚙️ Server-Based	⚙️ Server-Based	❌ None
Resource Footprint	🪶 Low (<2 GB RAM)	🔺 High	🔺 High	🔺 High	🪶 Very Low
Primary Use Case	🕵️ Portable Threat Hunting & Forensics	Enterprise SIEM	Enterprise Log Mgmt	Enterprise SIEM	Basic Log View